Наукові перспективи
Видавнича група

НАУКА і ТЕХНІКА СЬОГОДНІ

№ 1 (15)
2023

серія: право, серія: економіка, серія: педагогіка,
серія: техніка, серія: фізико-математичні науки

З Україною в серці!

Видавнича група «Наукові перспективи»

Громадська наукова організація «Всеукраїнська Асамблея докторів наук із державного управління»

Громадська організація «Асоціація науковців України»

«Наука і техніка сьогодні»

(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)

Випуск № 1(15) 2023

Київ – 2023

Publishing Group «Scientific Perspectives»

Public Scientific Organization «Ukrainian Assembly of Doctors of Sciences in Public Administration»

Public organization «Association of Scientists of Ukraine”

"Science and technology today"

("Pedagogy" series, "Law" series, "Economics" series, "Physical and mathematical sciences" series, "Technics" series)

Issue № 1(15) 2023

Kiev – 2023

ISSN 2786-6025 Online
УДК 001.32:1 /3](477)(02)

DOI: https://doi.org/10.52058/2786-6025-2023-1(15)

«Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)»: журнал. 2023. № 1(15) 2023. С. 314.

Згідно наказу Міністерства освіти і науки України від 07.04.2022 № 320 журналу присвоєно категорію "Б" із економіки та педагогіки
Згідно наказу Міністерства освіти і науки України від 06.06.2022 № 530 журналу присвоєно категорію "Б" із права
Згідно наказу Міністерства освіти і науки України від 10.10.2022 № 894 журналу присвоєно категорію "Б" із техніки (спеціальність - 122 Комп'ютерні науки)

Журнал видається за підтримки Міждержавної гільдії інженерів консультантів, Інституту філософії та соціології Національної Академії Наук Азербайджану (Баку, Азербайджан), громадської організації «Християнська академія педагогічних наук України» та громадської організації «Всеукраїнська асоціація педагогів і психологів з духовно-морального виховання»

Рекомендовано до видавництва Президією громадської наукової організації «Всеукраїнська Асамблея докторів наук з державного управління» (Рішення від 24.01.2023, № 5/1-23)

Журнал включено до міжнародної наукометричної бази Index Copernicus (IC), міжнародної пошукової системи Google Scholar та до міжнародної наукометричної бази даних Research Bible

17. Комнатний Сергій Олександрович - докторант кафедри філософії права та юридичної логіки Національної академії внутрішніх справ (Київ, Україна);

18. Кравчук Володимир Миколайович — доктор юридичних наук, доцент, доцент кафедри конституційного, адміністративного та міжнародного права Волинського національного університету імені Лесі Українки (Луцьк, Україна);

19. Кузьмич Людмила Володимирівна - доктор технічних наук, головний науковий співробітник Інституту водних проблем і меліорації Національної академії аграрних наук України (Київ, Україна);

20. Куницький Сергій Олегович - кандидат технічних наук, старший дослідник, провідний науковий співробітник науково-дослідної частини Національного університету водного господарства та природокористування (Рівне, Україна);

21. Лук'янчук Олександр Петрович — кандидат технічних наук, доцент, доцент кафедри будівельних, дорожніх, меліоративних, сільськогосподарських машин та обладнання Національного університету водного господарства та природокористування (Рівне, Україна);

22. Маджд Світлана Михайлівна - доктор технічних наук, професор , професор кафедри зеленої економіки та економіки природокористування Державної екологічної академії післядипломної освіти та управління (Київ, Україна);

23. Мануель Давид Массено - доцент відділу права та захисту даних, старший науковий співробітник і член координаційного комітету лабораторії UbiNET, запрошений член PDPC, член-консультант комісій цифрового права муніципальних адвокатських колегій Кампінаса та Прая-Гранде (Сан-Паулу), а також Комісії з інновацій, управління та технологій муніципальної адвокатської колегії Гуарульюса, коментатор IODA, почесний член IDEIA Institute, член Наукового комітету MICHR, член EDEN, член-кореспондент RedNAC, член UMAU, член-кореспондент UBAU (Португалія);

24. Микитин Тарас Миронович - кандидат технічних наук, завідувач кафедри економіки та менеджменту Рівненського державного інституту культури (Рівне, Україна);

25. Миргород-Карпова Валерія Валеріївна - кандидат юридичних наук, заступник директора з наукової роботи, старший викладач кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету (Суми, Україна);

26. Мізюк Вікторія Анатоліївна – кандидат педагогічних наук, доцент, декан факультету управління, адміністрування та інформаційної діяльності Ізмаїльського державного гуманітарного університету (Ізмаїл, Україна);

27. Мірошніченко Валентина Іванівна - доктор педагогічних наук, професор, завдувач кафедри психології, педагогіки та соціально-економічних дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького (Хмельницький, Україна);

28. Міхальський Томаш — доктор наук, доцент кафедри географії регіонального розвитку Гданського університету (Польща) ;

29. Огієнко Микола Миколайович - кандидат технічних наук, професор кафедри організації авіаційних робіт та послуг Національного авіаційного університету (Київ, Україна);

30. Одарченко Роман Сергійович - завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету (Київ, Україна);

31. Оніщенко Наталія Миколаївна - доктор юридичних наук, професор, Заслужений юрист України, академік НАПрН України, завідувач відділу теорії держави і права Інституту держави і права ім. В.М.Корецького НАН України (Київ, Україна);

32. Опанасенко Володимир Миколайович — доцент кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна);

33. Охріменко (Жмурко) Тетяна Олександрівна - старший науковий співробітник кафедри комп'ютеризованих систем управління Національного авіаційного університету (Київ, Україна);

34. Павлов Костянтин Володимирович — доктор економічних наук, професор, завідувач кафедри підприємництва і маркетингу Волинського національного університету імені Лесі Українки (Луцьк, Україна);

35. Поліщук Віталій Васильович — кандидат сільськогосподарських наук , завідувач відділу зрошення, відділення меліорації Інституту водних проблем і меліорації Національної академії аграрних наук України (Київ, Україна);

36. Приходькіна Наталія Олексіївна - доктор педагогічних наук, професор кафедри педагогіки, адміністрування і спеціальної освіти Навчально-наукового інституту менеджменту та психології ДЗВО «Університет менеджменту освіти» НАПН України (Київ, Україна);

37. Синиціна Юлія Петрівна - кандидат технічних наук, PhD, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ (Дніпро, Україна);

38. Сопілко Ірина Миколаївна - доктор юридичних наук, професор, Відмінник освіти України, Заслужений юрист України, декан юридичного факультету Національного Авіаційного Університету (Київ, Україна) ;

39. Стахова Анжеліка Петрівна — старший викладач кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна);

40. Турчинова Ганна Володимирівна — кандидат педагогічних наук, доцент, декан факультету природничо-географічної освіти та екології Національного педагогічного університету імені М.П. Драгоманова (Київ, Україна);

41. Федоренко Владислав Леонідович — доктор юридичних наук, професор, DrHb - доктор хабілітований наук правничих (Польська академія наук), Заслужений юрист України, директор Науково−дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України ((Київ, Україна);

42. Фесенко Андрій Олексійович - кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. (Київ, Україна);

43. Черненко Варвара Петрівна - кандидат фізико-математичних наук, доцент кафедри інформатики і вищої математики Кременчуцького національного університету імені Михайла Остроградського (Кременчук, Україна);

44. Чернуха Надія Миколаївна — доктор педагогічних наук, професор, професор кафедри соціальної реабілітації та соціальної педагогіки Київського національного університету імені Тараса Шевченка (Київ, Україна);

45. Чумак Оксана Володимирівна - доктор економічних наук, доцент, науковий співробітник відділу статистики і аналітики вищої освіти Державної наукової установи «Інститут освітньої аналітики», (Київ, Україна);

46. Шандра Наталія Андріївна - кандидат педагогічних наук, доцент кафедри іноземних мов для природничих факультетів Львівського національного університету імені Івана Франка (Львів, Україна);

47. Шеремет Інеса Володимирівна - кандидат педагогічних наук, доцент, доцент кафедри медикобіологічних та валеологічних основ охорони життя і здоров'я Національного педагогічного університету ім. М. П. Драгоманова (Київ, Україна);

48. Якимчук Олег Феодосійович - керівник групи білінгу Відділу бізнес-систем Департаменту інформаційних технологій ПРаТ «Рівнеобленерго» (Рівне, Україна);

49. Яцишин Андрій Васильович - доктор технічних наук, старший науковий співробітник, провідний науковий співробітник Відділу цивільного захисту та інноваційної діяльності Державної установи"Інститут геохімії навколишнього середовища Національної академії наук України" (Київ, Україна)

№ 1(15) 2023
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

ЗМІСТ

СЕРІЯ «Право»

СЕРІЯ «Економіка»

СЕРІЯ «Педагогіка»

СЕРІЯ «Техніка»

СЕРІЯ «Фізико-математичні науки»

УДК 354:328.185

https://doi.org/10.52058/2786-6025-2023-1(15)-238-256

Лебідь Олександр Васильович асистент кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет, вул. Сонячна, 3, м. Вінниця, 21008, тел.: (098) 888-26-06, https://orcid.org/0000-0003-4253-8696.

Кіпоренко Світлана Сергіївна асистент кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет, вул. Сонячна, 3, м. Вінниця, 21008, тел.: (097) 034-30-45, https://orcid.org/0000-0001-5045-5052.

Вовк Валерія Юріївна аспірантка, асистент кафедри комп'ютерних наук та економічної кібернетики, науковий співробітник наукових тематик, Вінницький національний аграрний університет, вул. Сонячна, 3, м. Вінниця, 21008, тел.: (068) 048-36-52, https://orcid.org/0000-0003-4029-5109.

ВИЯВЛЕННЯ КІБЕРАТАК ТА ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ТЕХНОЛОГІЇ НЕЙРОННИХ МЕРЕЖ В УМОВАХ КІБЕРВІЙНИ

Анотація. Сучасний світ рухається до того, що скоро неможливо буде обійтись без інтелектуальних систем інформаційної безпеки. Також стрімко зростає і перелік завдань інформаційної безпеки, вирішуваних із використанням інтелектуальних методів та засобів.

Найбільш актуальним завданням у сфері інформаційної безпеки, яка використовує методи та засоби штучного інтелекту, є виявлення вторгнень та атак на автоматизовані системи. Як свідчить існуючий досвід, досягнення прийнятних рівнів захисту інформаційних ресурсів від атак на систему не завжди можлива на основі існуючих алгоритмів та програмно-апаратних рішень. Сучасні ж засоби з виявлення атак повинні включати в себе, принаймні як складової частини, інтелектуальні підсистеми. Основою ж для цих підсистем є штучні нейронні мережі.

Обмін інформацією нині стає найактивнішою діяльністю у світі. Широке використання можливостей всесвітньої мережі, зростання та інтеграція корпоративних мереж у глобальні мережі загострює проблему інформаційній безпеці. Небезпека для корпоративної мережі з боку внутрішніх користувачів зростає. Проблема інформаційної безпеки виявлення кібератак є досить актуальною і пов'язана з наявністю вразливостей.

У статті подано короткий аналіз методів машинного навчання та нейромережевих технологій, які використовуються для виявлення аномалій. Було викладено матеріал щодо використання нейромережевих технологій у системах інформаційної безпеки. Запропоновано метод вирішення цього завдання на основі нейромереж з LSTM та FFN архітектурами. Наведено опис алгоритму та фрагментів програмної реалізації вказаного методу. Отримані в ході експериментів результати свідчать про можливість та доцільність застосування даного підходу для виявлення програмно-технічних впливів на критичні системи інформаційної інфраструктури в умовах кібервійни у масштабі часу, близькому до реального з високим рівнем достовірності.

Ключові слова: інформаційна безпека, кібератака, кібервійна, нейронні мережі, вразливість, програмне забезпечення, алгоритм.

Lebid Oleksandr Vasyliovych Assistant of the Department of Computer Sciences and Economic Cybernetics, Vinnytsia National Agrarian University, Soniachna St., 3, Vinnytsia, 21008, tel.: (098) 888-26-06, https://orcid.org/0000-0003-4253-8696.

Kiporenko Svitlana Sergiyivna Assistant of the Department of Computer Sciences and Economic Cybernetics, Vinnytsia National Agrarian University, Soniachna St., 3, Vinnytsia, 21008, tel.: (097) 034-30-45, https://orcid.org/0000-0001-5045-5052.

Vovk Valeriia Yuriivna Postgraduate student, assistant of the Department of Computer Sciences and Economic Cybernetics, researcher of scientific topics, Vinnytsia National Agrarian University, Soniachna St., 3, Vinnytsia, 21008, tel.: (068) 048-36-52, https://orcid.org/0000-0003-4029-5109.

DETECTING CYBER ATTACKS AND IMPROVING INFORMATION SECURITY BASED ON TECHNOLOGY OF NEURAL NETWORKS IN THE CONDITIONS OF CYBERVIYNA

Abstract. The modern world is moving towards the fact that soon it will be impossible to do without intelligent information security systems. The list of information security tasks solved using intelligent methods and tools is also growing rapidly.

The most urgent task in the field of information security, using methods and tools of artificial intelligence, is the detection of intrusions and attacks on automated systems. As the existing experience shows, it is not always possible to achieve acceptable levels of protection of information resources from attacks on the system based on existing algorithms and software and hardware solutions. Modern tools for

detecting attacks should include, at least as an integral part, intelligent subsystems. The basis for these subsystems are artificial neural networks.

The exchange of information is now becoming an active activity in the world. The widespread use of the world wide web, the growth and integration of corporate networks into global networks exacerbates the problem of information security. The danger of the corporate network from internal users is growing. The problem of information security of detecting cyber attacks is quite relevant and is associated with the presence of vulnerabilities.

The article presents a brief analysis of machine learning methods and neural network technologies that are used to detect anomalies. Material on the use of neural network technologies in information security systems was presented. A method for solving this problem based on neural networks with LSTM and FFN architectures is proposed. A description of the algorithm and fragments of the software implementation of this method is presented. The results obtained during the experiments indicate the possibility and expediency of using this approach to identify software and hardware impacts on critical systems of information infrastructure in a cyber war on a time scale close to real with a high level of reliability.

Keywords: information security, cyber attack, cyber war, neural networks, vulnerability, software, algorithm.

Постановка проблеми. Сучасні наукові досягнення у таких галузях інформатики, як математичне моделювання стану зовнішнього світу, штучний інтелект, теорія прийняття рішень, обробка зображень, сигналів і сцен розпізнавання образів, оптимальне управління та інших дозволяють говорити про реальну можливість переходу до нового покоління засобів інформаційного захисту – інтелектуальних систем інформаційної безпеки. Стрімко зростає і перелік завдань інформаційної безпеки, які вирішуються з використанням інтелектуальних методів та засобів. Першим найбільш актуальним завданням у сфері інформаційної безпеки, яке потребує використання потужного арсеналу методів та засобів штучного інтелекту, є виявлення кібератак на автоматизовані інформаційні системи в умовах кібервійни.

Останні геополітичні події серйозно переформатували IT-галузь. З 24 лютого 2022 року українські організації, незалежно від їхньої величини, піддаються безпрецедентним за своїм розмахом та інтенсивністю кібератакам. Зловмисники атакують буквально все, до чого можуть дістати, орієнтуючись на українські IP-адреси. Найбільшого поширення набули DDoS-атаки, злом великих компаній із подальшою крадіжкою інформації, а також дефейс популярних ресурсів. Під прикриттям шквалу масових атак, продовжують діяти кіберзлочинці, націлені на великі компанії (державний сектор,

банківську сферу, паливно-енергетичний комплекс, інформаційну галузь, наукові інститути та організації тощо).

У даний час технології машинного навчання та нейромереж застосовуються для вирішення безлічі завдань класифікації, прогнозування та прийняття рішень. У системах кіберзахисту ці технології використовуються для виявлення закономірностей у поведінці систем, виявлення аномальної поведінки та протидії комп'ютерним атакам.

Аналіз останніх досліджень і публікацій. Опис прикладів та способів застосування нейромережевих технологій для виявлення загроз інформаційній безпеці представлено в низці наукових робіт зарубіжних та вітчизняних науковців: Liu Hua Yeo, Xiangtong Che, Shalini Lakkaraju [1], Jain G., Sharma M., Agarwal B. [2]. Хорошко В.О., Ткач Ю.М., Шелест М.Є. [3], Довбиш А.С., Ободяк В.К., Шелехов І.В. [4], Рогоза П., Єсін В. [5], Курбан О.В. [6] та ін.

Мета статті – розробити модельне, алгоритмічне та програмне забезпечення для виявлення в режимі реального часу спроб порушення коректного функціонування систем критичної інформаційної безпеки в умовах кібервійни.

Виклад основного матеріалу. У матеріалах, опублікованих американською компанією Check Point5, сказано, що 2022 рік почався з масованої експлуатації однієї з найсерйозніших вразливостей в Інтернеті – Apache log4j і продовжився повномасштабною кібервійною з початком «російської спеціальної військової операції» в Україні. Також зазначається, що основними цілями атак є сектор освіти та досліджень, зростання яких склало 53% порівняно з 2 кварталом 2021 року, в середньому відбулось понад 2,3 тис. атак на такі організації щотижнево. Наступними за кількістю здійснених кібератак є урядовий та військовий сектори, де у середньому протягом тижня відбувалося 1,6 тис. атак, що на 44% більше у порівнянні з аналогічним періодом 2021 року. Далі йдуть сектори інтернет-провайдерів та MSP, охорони здоров'я та зв'язку – у середньому на організації такого типу припадає 1,3 тис. атак на тиждень, що вдвічі перевищує показник 2021 року [7].

У публікаціях Європейського агентства з кібербезпеки (European Union Agency for Cybersecurity, ENISA) зазначено, що все більш активну участь у розробці та застосуванні кіберзброї приймають урядові організації та спецслужби [8].

У відомих підходах до процесу виявлення мережевих кібератак у локальних мережах використовують деяку форму аналізу на основі правил, які ґрунтуються на наборі заздалегідь сформованих рекомендацій, наданих адміністратором чи автоматично створених системою. Однак, такі системи правил вимагають постійного оновлення для того, щоб залишатися актуальними, при чому час до застосування правил оновлення системи є досить невизначеним. Вони страждають і від нездатності виявляти сценарії

кібератак, які можуть відбуватися протягом тривалих періодів часу. Будь-який поділ кібератаки або в часі, або серед кількох, незв'язаних між собою систем, значно ускладнює її виявлення із використанням цих методів.

Постійне вдосконалення технологій та засобів реалізації кібератак щодо критичних систем інформаційної безпеки в умовах кібервійни зумовлює нагальну необхідність створення адекватних чи переважаючих методів та засобів захисту від них. Сьогодні для захисту критичних систем інформаційної інфраструктури (далі – КСІІ) від програмно-технічних впливів (далі – ПТВ) використовуються міжмережові екрани (далі – МЕ), системи виявлення та попередження вторгнень (IDS/IPS), системи запобігання втраті даних (DLP, Data Loss Prevention), системи управління подіями інформаційної безпеки (SIEM, Security information and event management), антивіруси та інше.

Сучасні методи виявлення програмно-технічних впливів, що призводять до інцидентів інформаційної безпеки, можна розділити на дві основні категорії: розпізнавання зловживань та виявлення аномалій. Методи розпізнавання зловживань, які описуються за допомогою сигнатур відомих кібератак, мають високу точність та низький рівень хибних спрацьовувань, але не здатні виявляти кібератаки, для яких відсутні сигнатури. Методи виявлення аномалій дозволяють ідентифікувати раніше невідомі кібератаки, але мають високий рівень хибних спрацьовувань.

Нейронні мережі є альтернативою компонентам статистичного аналізу систем виявлення аномалій. Нейромережі дозволяють відслідкувати типові характеристики мережного трафіку та ідентифікувати статистично значущі відхилення від встановленого режиму роботи. Вони застосовуються як статистична система виявлення зловживання через їхню здатність до самонавчання. Більше того, нейромережу можна налаштувати так, щоб вона і надалі самостійно вдосконалювалася, постійно реагуючи на найменші зміни в локальній мережі.

Так, наприклад, методи розпізнавання образів, що базуються на сигнатурному аналізі, мають високу точність і низький рівень помилкових спрацьовувань, але вони нездатні виявляти кібератаки, в яких відсутні сигнатури. Методи виявлення аномалій дозволяють виявляти раніше невідомі кібератаки, проте мають високий рівень хибних спрацьовувань, зумовлених складністю розробки профілів нормальної поведінки контрольованих систем. Оптимальним рішенням може бути комплексне використання даних технологій із огляду на той факт, що результати, отримані за допомогою методів виявлення аномалій, можуть використовуватися для розробки нових сигнатур.

Найбільшою перевагою підходу, заснованого на аномаліях, є його здатність виявляти кібератаки нульового дня, оскільки він не залежить від використовуваної бази даних сигнатур, а дозволяє виявляти відхилення від

нормальної поведінки. Поведінка кожної цільової системи є унікальною, тому підходи, засновані на виявленні аномалій, повинні використовувати індивідуальні профілі, які, у свою чергу, ускладнюють зловмиснику точне визначення того, які дії він може виконати, не викликаючи тривоги. Недоліками систем виявлення кібератак, заснованих на виявленні аномалій, в умовах кібервійни є: високий рівень хибнопозитивних результатів та необхідність формування профілів нормальної поведінки контрольованої системи [1].

На рис. 1. наведено класифікацію та коротку характеристику методів глибокого навчання, які використовуються для відстеження вторгнень за допомогою виявлення аномалій.

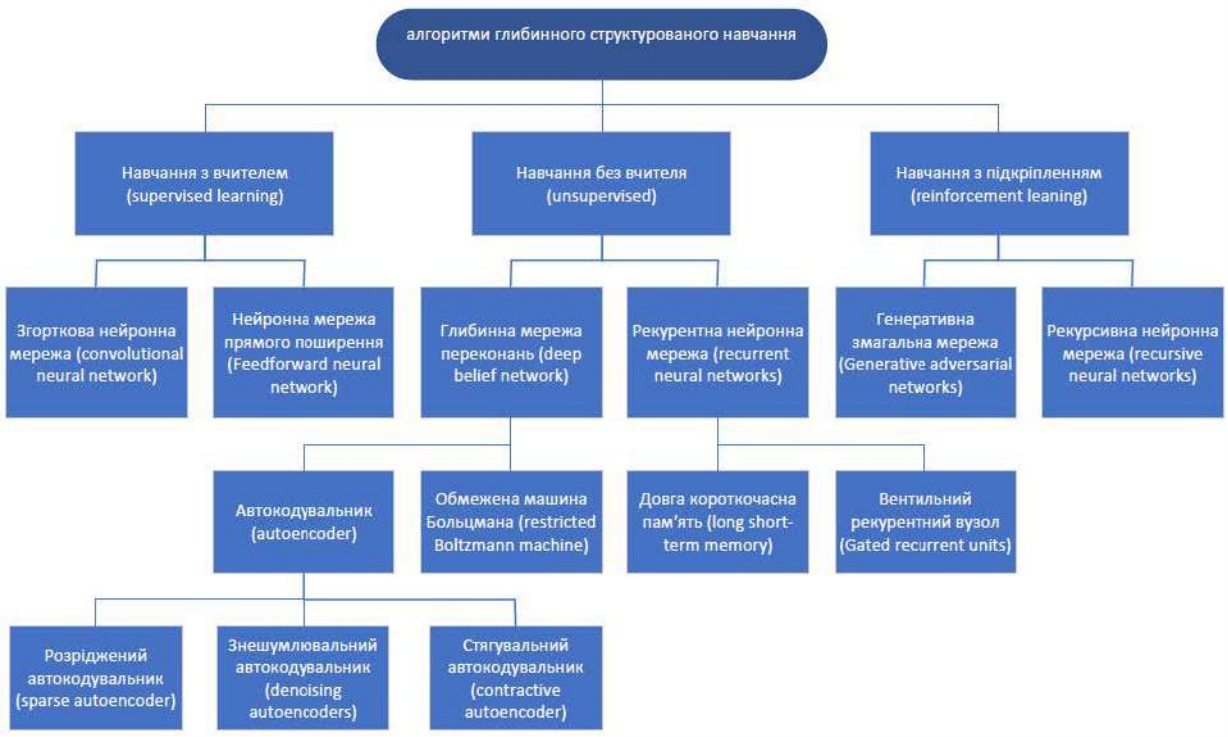

Рис. 1. *Класифікація методів глибокого навчання, що використовуються для встановлення вторгнень за допомогою виявлення аномалій*

Джерело: побудовано авторами на основі власних досліджень

На основі проведених досліджень було визначено, що технології DL доцільно застосовувати на більших обсягах даних для неконтрольованого або напівкерованого вивчення та встановлення зв'язків та закономірностей у процесах та подіях, а також обґрунтовано такі характеристики якості методів виявлення кібератак на інформаційне середовище в умовах кібервійни, як точність (precision), чутливість (sensitivity), середнє гармонійне значення точності та відгуку (F1-score), крива ROC (receiver operating) characteristic), що

описує компроміс класифікатора між правильно-позитивними (true positive) та хибно-позитивними (false positive) рішеннями, характеристика продуктивності AUC (area under curve ROC), наведено характеристики точності ML і DL алгоритмів виявлення кібератак із бази даних NSL-KDD '99 [2].

У ряді джерел пропонується для виявлення аномалій за невідомими даними використовувати генеративно-змагальні мережі (Generative Adversarial Networks, GAN). Вказана модель застосовувалася для експериментального дослідження набору даних ботнетів ISCX [9]. Окрім того, для виявлення аномалій застосовується модель на основі двоспрямованої GAN (BiGAN), яка додатково проводить зворотне відображення реальних даних у прихований простір. Крім економії часу, BiGAN сприяє більш ефективному вилученню ознак мережного трафіку. Ця модель на наборі даних KDD Cup 99 показує точність на 93,24% [10].

На основі опрацьованих публікацій було визначено, що одним із найбільш перспективних підходів до виявлення кібератак у режимі часу, близькому до реального, є використання рекурентних нейронних мереж (Recurrent Neural Network, RNN) [10; 11]. Відмінною особливістю RNN є зворотній зв'язок, який дозволяє аналізувати послідовні дані, такі як тимчасові лави. Аналізуючи послідовність вимірювань різних параметрів поточного процесу, нейромережа навчається передбачати його стан у майбутніх періодах. Якщо передбачений стан RNN відрізняється від поточного, реєструється аномалія. RNN застосовується для бінарної та мультикласової класифікації наборів мережевих даних NSL-KDD. Недоліком стандартних RNN є проблеми зі зникненням градієнта та нестача пам'яті для використання інформації за попередні моменти часу [11].

Проведений аналіз показав, що одним із найперспективніших підходів до виявлення аномальної поведінки контрольованих КСІІ у режимі реального часу є застосування методів глибокого навчання, зокрема, рекурентних мереж LSTM. Основними проблемними є питання, пов'язані з побудовою профілів нормальної поведінки контрольованих систем, визначення параметрів та налаштування нейромережі, забезпечення її адаптованості до мінливих умов.

Нинішня ситуація вимагає негайної реакції та приведення систем інформаційних технологій (далі – ІТ) та інформаційної безпеки (далі – ІБ) у режим посиленого захисту.

У зв'язку з вторгненням російської федерації на територію України, загальна кількість звернень за сервісами захисту склала щонайменше третину від усіх запитів 2021 року, і продовжує зростати, велика кількість звернень надходить як від атакованих компаній, так і від тих, хто хоче підвищити рівень своєї захищеності, щоб не стати черговою жертвою.

На основі проведеного аналізу було досліджено алгоритм виявлення подій інформаційної безпеки (далі – ПІБ), зумовлених програмно-технічним

впливом (далі – ПТВ) на КСІІ, за допомогою нейромереж з LTSM та FFN архітектурами. Ці нейромережі забезпечують вирішення завдання регресії, тобто прогнозування значень параметрів, що характеризують рівень небезпеки ПТВ для системи, яка зазнає кібератак. Розроблений на їх основі алгоритм забезпечує виявлення аномалій та ранніх ознак ПТВ, які можуть призвести до інцидентів інформаційної безпеки.

Під ПТВ розуміється цілеспрямований апаратно-програмний або програмний вплив, а також їх комбінація на КСІІ, які призводять до порушення процесу їх функціонування [6]. За допомогою нейромережі формується значення вихідної змінної, що характеризує рівень або ступінь небезпеки для КСІІ виявленого ПТВ в умовах кібервійни (табл. 1).

Таблиця 1

Рівень небезпеки для критичних систем інформаційної інфраструктури виявленого програмно-технічного впливу

№ з/п	Рівень небезпеки	Опис
1	Не враховується	короткочасне порушення в роботі інформаційної інфраструктури, що не впливає на процес передачі та обробки даних, спричинене поодинокими збоями
2	Прийнятний	порушення, які мають одиничний характер і не взаємопов'язані один з одним
3	Небажаний	порушення, що значно впливають на процес передачі або обробки даних, спричинені збоями
4	Неприйнятний	навмисні (у тому числі циклічні) програмно-технічні впливи на критичні системі інформаційної інфраструктури, що призводять до подій інформаційної безпеки

Джерело: узагальнено авторами на основі проведених досліджень

Схема алгоритму виявлення аномальної поведінки систем, зумовлених програмно-технічними впливами на основі технології нейромереж представлена на рис. 2.

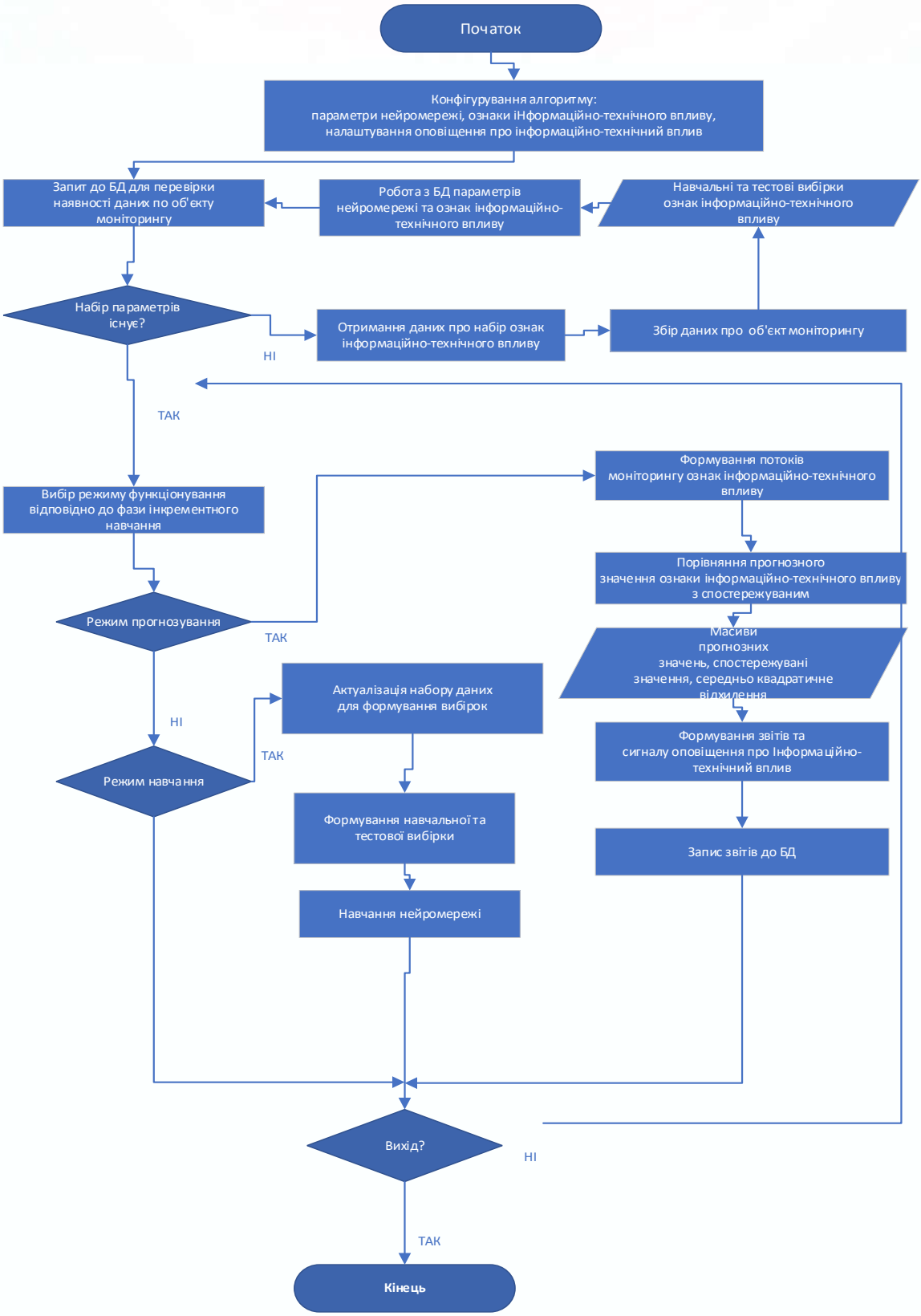

Рис. 2. *Схема алгоритму аномальної поведінки систем із використанням технології нейромережі*

Джерело: власна розробка авторів

Основними етапами алгоритму виявлення аномальної поведінки систем є:

- визначення набору вхідних змінних нейромережі, вихід числових значень які за встановлені межі трактуються як ознаки ПТВ та СІБ;
- збирання та отримання даних про контрольований об'єкт;
- навчання нейромережі;
- прогнозування та виявлення аномальної поведінки.

Працездатність алгоритму виявлення аномалій залежить від коректності вибору набору вхідних змінних нейромереж, вихід числових значень яких за встановлені межі трактується як ознаки ПТВ та СІБ. Алгоритм призначений для виявлення аномалій, викликаних ПТВ на вузол інформаційної інфраструктури, яка підтримує мережеві сервіси: сервер QoS, сервер прикладних служб HTTP, FTP, SMTP, SNMP та інші. Відповідно, як ознаки можуть використовуватися: кількість активних процесів; дані про активні (нові, віддалені, змінені) облікові записи користувачів; дані про мережеві з'єднання та запити; зміни у записах системних планувальників; дані про процеси та демони (запуск, зупинка); ступінь завантаженості процесора; дані щодо використання пам'яті. Аномальні зміни значень даних ознак сигналізують про несанкціоновану активність користувачів програмно-технічного впливу та функціонування шкідливого програмного забезпечення (далі – ШПЗ).

На етапі конфігурування алгоритму формується набір параметрів, необхідних для його успішного функціонування з врахуванням особливостей об'єкта, що підлягає аналізу. До основних параметрів відносяться: тимчасовий ряд, який характеризує ознаки ПТВ (один або кілька); граничні значення вихідної змінної, що відповідає за формування оповіщення про ПТВ або СІБ; варіанти функції втрат (loss function); процедури оптимізації (optimization procedure).

На початку експериментального відпрацювання доцільно використовувати стандартну функцію втрат, що є сумою квадратичних помилок (sum of squared errors, SSE). Для оптимізації використовуються оптимізатори RMSProp та Adam (Adaptive Moment Estimation) з пакету Keras – відкрита нейромережна бібліотека, написана мовою Python. У процесі конфігурування формується структура нейромережі. Ця операція виконується відповідно до послідовності, прийнятої для бібліотеки, що використовуються, у нашому випадку Tensorflow та Keras [12; 13]

Бібліотека Keras надає можливість роботи з кількома типами RNN: шари класів keras.layers.SimpleRNN, keras.layers.GRU, keras.layers.LSTM. Для розв'язання завдання виявлення аномалій за допомогою прогнозування часового ряду використовуються шари LSTM. Навчання LSTM мережі здійснюється на тренувальному наборі, який включає один або кілька часових рядів відповідно до кількості вхідних параметрів нейромережі, представлених

у вигляді пар вхідних та вихідних послідовностей.

У деяких ситуаціях виникає необхідність представлення наборів даних для двох рядів незалежних величин (два незалежні параметри) та однієї залежної величини із необхідністю прогнозування всіх трьох рядів. У цьому випадку модель LSTM модифікується до багатовимірної моделі LSTM для кількох серійних входів (Multiple Input Series) або моделі LSTM для декількох паралельних серій (Multiple Parallel Series) [12].

В обох випадках представлення наборів даних, вхідний шар мережі перетворюється відповідно до їх розмірності:

LSTM(units=32, activation='relu', input_shape=(n_steps, n_features)

У другому випадку модифікується і вихідний повнозв'язний шар відповідно до розмірності даних:

model.addELayer (Dense(n_features)),

n_features = X.shape– кількість вхідних незалежних рядів метрик;

n_steps = 100 – кількість елементів у n-грамі [1].

При формуванні навчального та тестового набору даних проводиться нормалізація даних. Процедура нормалізації мовою Python виглядає наступним чином:

```
def normalize(result):
  result_mean = result.mean() # обчислення
середнього значення набору даних
      result_std = result.std() #
обчислення стандартного відхилення
result -= result_mean
result /= result_std
return result, result_mean
```

Для перевірки працездатності алгоритму та коректності моделі нейромережі розроблено програму виявлення СІБ та ПТВ мовою Python3. У ході експериментів використовувалася нейромережа з архітектурою «стекова LSTM» з наступною структурою:

- кількість елементів у n-грамах – 100;
- кількість шарів – 3;
- перший шар за кількістю нейронів відповідає довжині вхідної послідовності (n-1), коефіцієнт перенавчання Dropout = 0,2;
- другий шар LSTM – 130 нейронів з коефіцієнтом перенавчання = 0,2;
- третій шар LSTM – 100 нейронів;
- вихідний шар, що складається з одного нейрона, повнозв'язний (клас Densely-connected) з лінійною функцією активації.

У результаті експериментів підтверджено, що дана структура нейромережі у процесі роботи алгоритму забезпечує вирішення задач прогнозування та виявлення аномалій для одного контрольованого параметра. Для обробки кількох параметрів необхідно змінити структуру нейромережі відповідно до наведених вище рекомендацій. При проведенні експериментів

як вихідні дані були використані:

- тимчасовий ряд, що містить дані про завантаженість процесора протягом 660 секунд (дані отримані з середовища osquery з використанням Python$_3$ bindings – osquery-python);

- тимчасовий ряд, який містить 660 значень, дані в якому відповідають часу відповіді сервера HTTP, що формується за нестандартним законом розподілу: у 2/3 випадків генеруються числа [0; 0,5) потім зменшується з ймовірністю [0,5; 1); аномальні дані відповідають розподілу Гауса в діапазоні [0,9; 1) [12].

Опис початкової структури LSTM мережі для реалізації алгоритму мовою Python$_3$ з використанням бібліотек Tensorflow та Keras має такий вигляд:

```
def generate_model():
    model = Sequential()
  # Перший шар відповідає довжині вхідної послідовності
model.add(LSTM(input_shape=(sequence_
length-1,1),
      units=32,return_sequences=True))
      model.add(Dropout(0.2)) # виняток
перенавчання
  # Другий шар LSTM із 128 нейронів
model.add(LSTM(units=128, return_
sequences = True))
      model.add(Dropout(0.2))
  # Третій LSTM шар із 100 нейронів
model.add(LSTM(units=100, return_
sequences = False))
   model.add(Dropout(0.2))
  # Повнозв'язний вихідний шар з лінійною
ФА
  model.add(Dense(units=1))
  model.add(Activation('linear'))
  алгоритм оптимізації, функція втрат
    model.compile(loss=’mean_squared_
error', optimizer='rmsprop')
  return model
```

Для формування навчального та тестового наборів передбачена функція split_sequence, вхідними параметрами для якої є: масив даних, що містить часовий ряд параметра, точка початку тренувального набору в масиві даних, точка закінчення тренувального набору, точка початку тестового набору, кінцева точка тестового набору. Нижче наведено фрагмент функції, в якому представлені основні операції з формування тренувального та тестового наборів:

```
train_end, test_start, test_end):
  result = [] # масив н-грам
діапазон можна задати і як довжина дата
мінус sequence_length
  for index in range(train_start, train_
end - sequence_length):
  result.append(data[index: index +
sequence_length])
  result = np.array(result)
```

```
  result, result_mean = normalize(result)
  prin ("Розмірність масиву TH:",
result.shape)
  train = result[train_start:train_end, :]
  np.random.shuffle(train)
  X_train = train[:, :-1]
  y_train = train[:, -1]
  # Аналогічно - формування тестового
набору
 …
  X_test = resultt[:, :-1] # Відділяємо
вибірки від міток, ВИБІРКА
  y_test = resultt[:, -1] # МІТКИ
 …
return X_wtrain, y_wtrain, X_wtest, y_
wtest
```

У ході перевірки працездатності моделі мережі в обох випадках набори формувалися наступною командою, що визначає їх розмірність:

```
X_train, y_train, X_test, y_test = prepare_data(rez, 0, 600, 400, 660)
```

Метод дозволяє реалізувати безперервний процес обробки даних у реальній системі виявлення ПТВ шляхом чергування циклів прогнозування (наприклад, побудова прогнозу на 60-хвилинний інтервал через кожні 30 хвилин) та тренування моделі за допомогою накопичених даних (використовуються дані за попередні 24 години). Порівняння прогнозованого значення параметра та його значення, що спостерігається, а також моніторинг статистичної метрики – індикатора аномалії, проводяться щохвилини. Необхідна тимчасова послідовність уточнюється та формується за результатами відпрацювання моделі на стенді. За результатами роботи програми було сформовано графіки, які відображають зміну часу значення контрольованої величини (рис. 3).

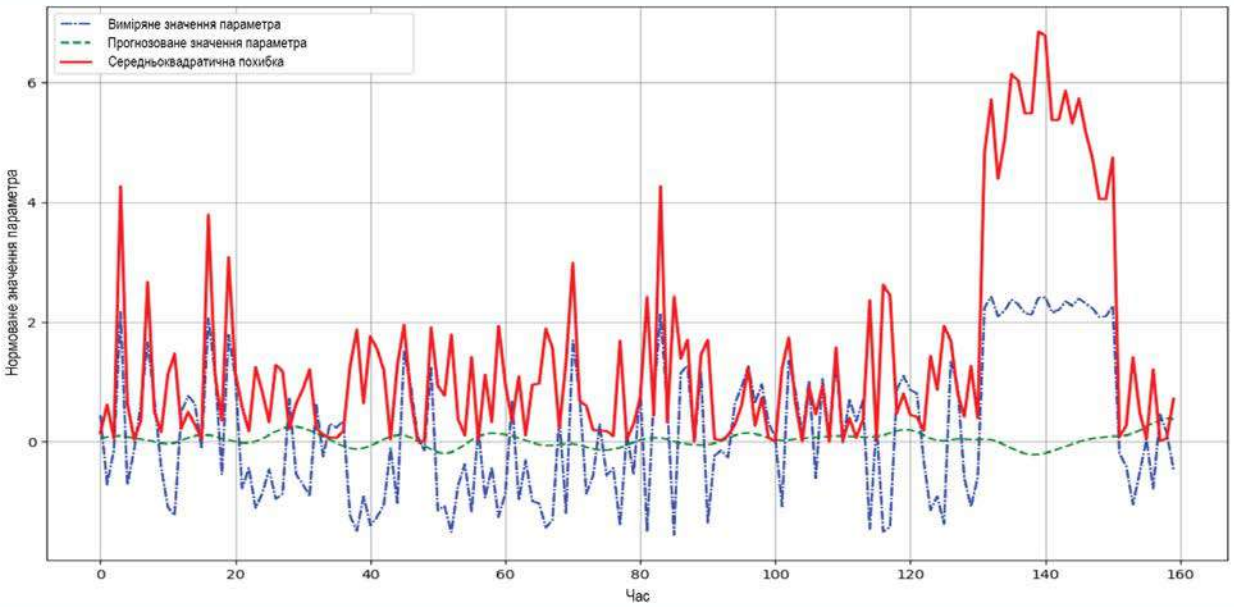

Рис. 3. *Графіки часу відповіді сервера HTTP та Середньоквадратичного відхилення фактичного значення параметра від прогнозованого*

Джерело: побудовано авторами на основі проведених досліджень

Отже, судячи з графіка, модель нейромережі дозволяє однозначно фіксувати аномалію.

Як метрика-індикатор аномалії використовується значення середньоквадратичної помилки (далі – СКП), що характеризує ступінь відхилення виміряного фактичного рівня параметра від прогнозованого. Подані графіки дозволяють візуально визначити аномалію контрольованого параметра викиду значення метрики-індикатора, яке оцінюється на заданому часовому інтервалі (15-20 вимірювань, 15-20 секунд). З практики застосування статистичних метрик випливає, що відхилення метрики-індикатора більш ніж у 2-3 рази від середнього значення інтервал-прогнозу (160 тестових значень) є ознакою аномалії. Для виявлення аномалії в часовому ряду контрольованої величини (завантаження процесора, обсяг споживаної оперативної пам'яті та інше) при експериментальному відпрацюванні алгоритму можна використовувати стандартне відхилення і середнє абсолютне відхилення (median absolute deviation – MAD).

Незважаючи на те, що очевидний тренд у зміні ознаки (час відповіді сервера HTTP) відсутній, тестовий та навчальні набори насичені викидами, квадратичне відхилення для нормалізованої величини коливається в інтервалі [0;0,4].

Як вихідні дані для формування навчального та тестового набору використовується знову згенерований часовий ряд параметра часу відповіді сервера HTTP із значними викидами та відсутністю тренду. Починаючи з 630 секунд у даних виявлена аномалія.

На рис. 4-5 представлені вихідні дані та результати повторного експерименту.

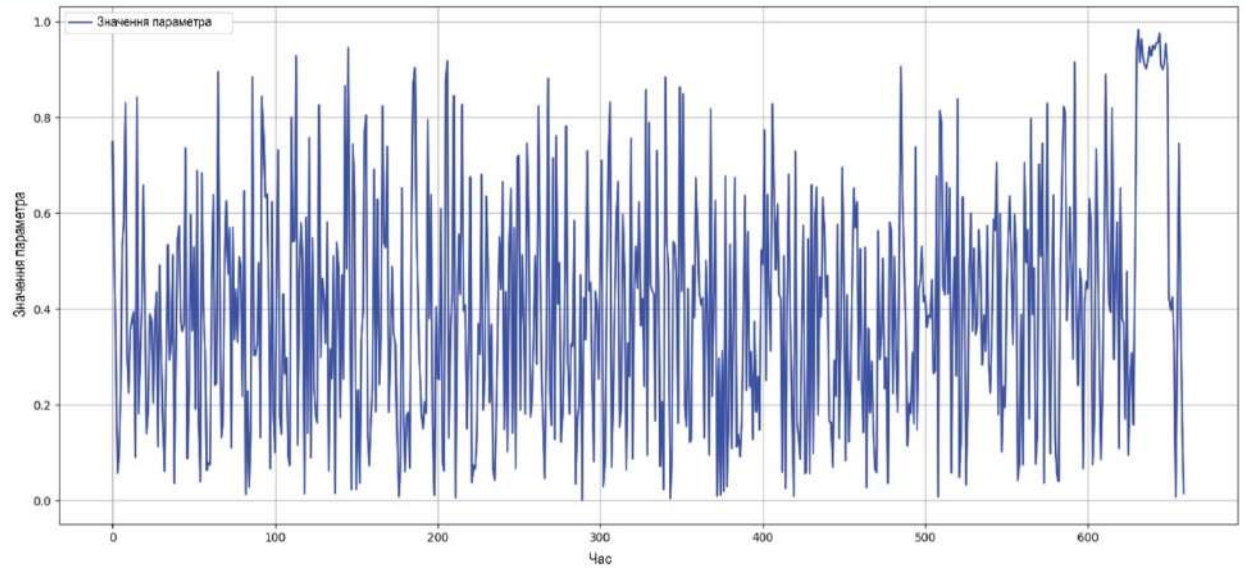

Рис. 4. Вихідний набір даних для формування тестової та навчальної вибірки (час відповіді сервера HTTP, 660 вимірів, 660 секунд)

Джерело: побудовано авторами на основі проведених досліджень

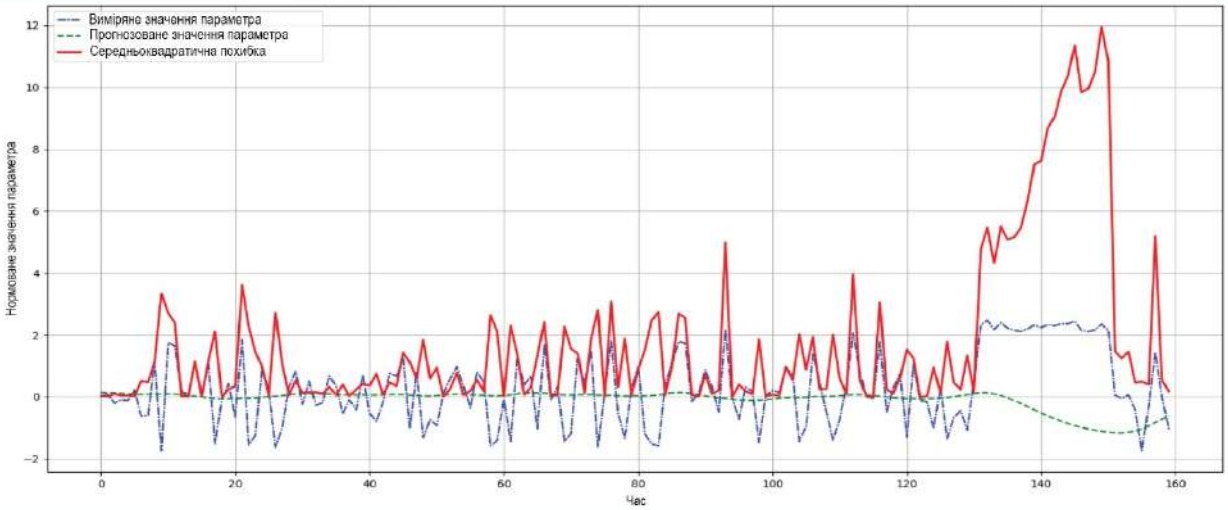

Рис. 5. *Графіки часу відповіді сервера HTTP та Середньоквадратичного відхилення фактичного значення параметра від прогнозованого*
Джерело: побудовано авторами на основі проведених досліджень

Розглянута вище модель нейромережі є єдиною на вирішення завдань виявлення аномалій і програмно-технічних впливів. Проведені дослідження показали, що після закінчення процесу навчання нейромережі (950 епох) середньоквадратична помилка (MSE), яка використовується як функція втрат при навчанні нейромережі, склала 0,0004-0,0013, що свідчить про високий рівень налаштування нейромережі.

На рис. 6 представлено, вихідний набір даних для формування тестової та навчальної вибірок, а також ступінь використання процесора в 660 вимірів. У дані внесена аномалія, починаючи з 600 секунди. При цьому є явний тренд у змінах значень ознаки.

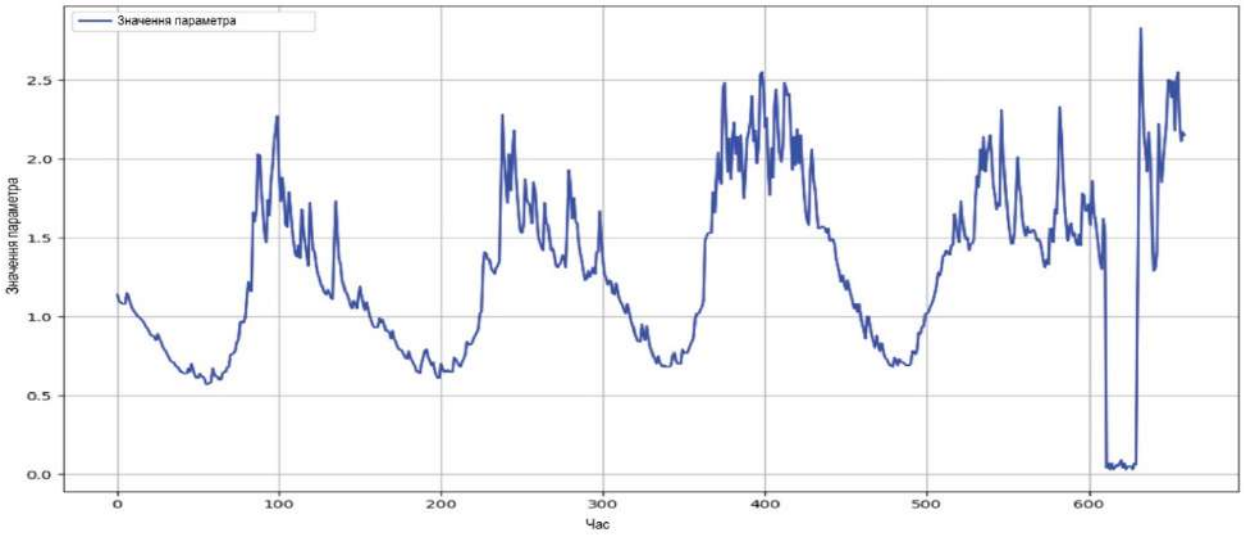

Рис. 6. *Вихідний набір даних для формування тестової та навчальної вибірок – ступінь використання процесора, 660 вимірів*
Джерело: побудовано авторами на основі проведених досліджень

На рис. 7 зображено результат моделювання роботи алгоритму зі зазначеною вище структурою мережі на наборі даних, які наведені на рис. 6.

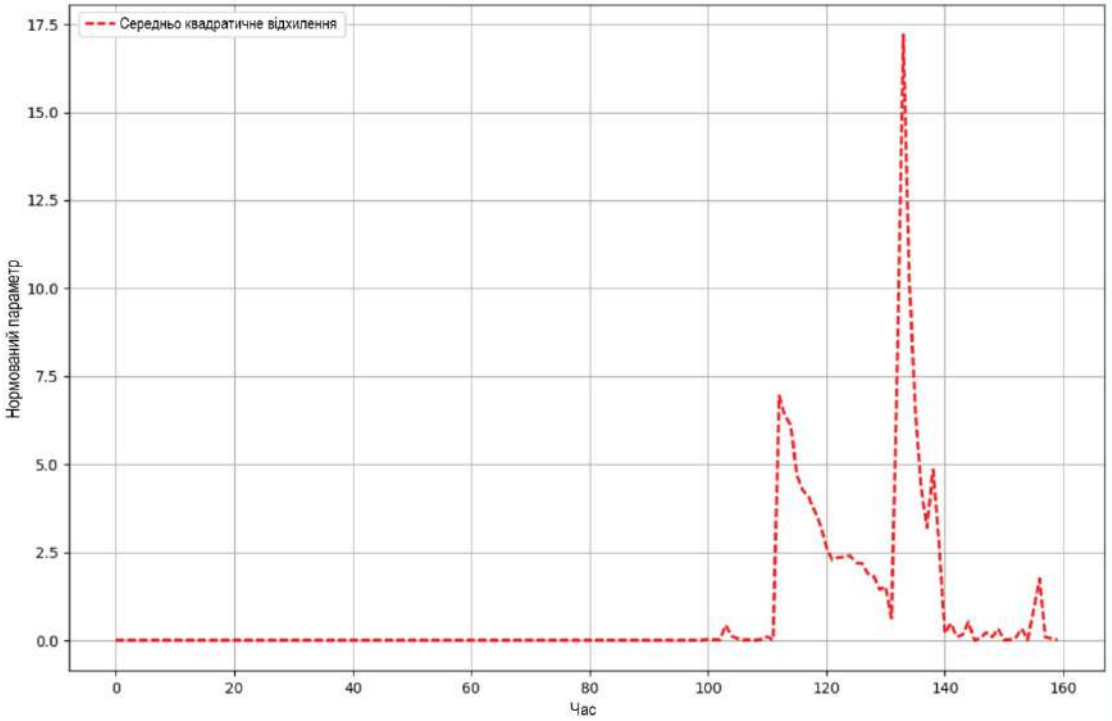

Рис. 7. *Результати моделювання роботи алгоритму виявлення аномалій із використанням FFN нейромережі*

Джерело: побудовано авторами на основі проведених досліджень

Результати проведених експериментів показали, що представлений у статті метод виявлення кібератак інформаційній безпеці за допомогою нейронних мереж в умовах кібервійни, його алгоритмічна та програмна реалізації дозволяють вирішити задачу виявлення аномальної поведінки контрольованих систем за допомогою прогнозування і моніторингу аналізованих параметрів, вихід значень яких за встановлені межі є ознакою ПТВ та СІБ. Важливою перевагою даного підходу є можливість адаптації нейромережі у разі зміни режиму та умов функціонування системи.

Російсько-українська війна з початку повномасштабного вторгнення показала, що кібератаки агресора збігаються з військовими атаками, тобто захоплення або знищення об’єктів критичної інфраструктури. Слід зазначити, що країна-агресор використовує хакерські атаки для підтримки свого масштабного наступу на Україну, поєднуючи зловмисне програмне забезпечення з ракетами в кількох атаках, зокрема на телевізійні станції та державні установи.

Загроза кібератак росії на українські системи та європейських партнерів залишається високою, оскільки концепція російської гібридної війни передбачає використання різноманітних впливів проти України.

Масова кібератака на українські державні установи та бізнес почалася задовго до військового вторгнення. За даними Міністерства цифрової трансформації України, з початком бойових дій 24 лютого 2022 року їх кількість подвоїлася з приблизно 200 на місяць до понад 400 [14]. У Держспецзв'язку та захисту інформації заявили, що кібератаки стали невід'ємною частиною ведення війни, що дістало назву кібервійни. Згідно з цими даними, з початку року рф запустила кілька сімейств шкідливого програмного забезпечення в Україні.

Загрози у кіберпросторі є найбільш серйозними для національної безпека України. Зараз кібербезпека є критичною проблемою в усіх аспектах економіки, політики, суспільства та армії. Проте, дана загроза є однією з найменш відомих і найбільш недооцінених. Тому необхідно розуміти, що кіберпростір є найважливішим театром бойових дій сьогодні. Боротьба за кібердомінування – і, як результат, здатність протистояти кібератакам – відкриває нову еру суперницьких відносин, які докорінно змінять характер і структуру збройних сил. Слід також зазначити, що кібербезпека не може бути досягнута на національному рівні. Це потребує спільних зусиль приватного сектору та бізнесу, а також міжнародної координації та співпраці в безпрецедентних масштабах.

Сьогодні, найточнішим методом виявлення кібеатак в інформаційному просторі в умовах кібервійни є метод, що ґрунтується на сигнатурному аналізі, який добре функціонує при виявленні вже відомих кібератак, але абсолютно не придатний для виявлення нових, раніше невідомих. І, як свідчить практика, саме нові, раніше невідомі кібератаки є причиною глобальних інформаційних катастроф і призводять до значних збитків.

Порівняно з традиційними нейронними мережами, перспективним є використання глибоких нейронних мереж із ефективним нелінійним перетворенням і представленням даних. Така мережа виконує глибоке ієрархічне перетворення вхідного простору. Завдяки багаторівневій архітектурі глибокі нейронні мережі дозволяють обробляти та аналізувати великі обсяги даних, а також моделюють когнітивні процеси у різних областях. Зараз більшість високотехнологічних компаній США (Microsoft, Google, Facebook, Baidu та інші) використовують глибокі нейронні мережі для проєктування різноманітних інтелектуальних систем. На думку вчених Массачусетського технологічного інституту, глибокі нейронні мережі увійшли до списку 10 найперспективніших високих технологій, здатних кардинально змінити повсякденне життя більшості людей на нашій планеті у найближчому майбутньому. Глибоке навчання стало однією з найбільш затребуваних сфер інформаційних технологій.

Висновки. Представлені у статті моделі, алгоритм та програмне забезпечення призначені для автоматизації процесів виявлення кібератак

інформаційної безпеки та програмно-технічних впливів на КСІІ в умовах кібервійни. Метод та алгоритм реалізовані у вигляді програм мовами $Python_3$ та Go з використанням пакетів Keras, Tensorflow, osquery, go-deep.

Результати експериментів підтвердили працездатність даного підходу та доцільність його застосування для виявлення кібератак у реальному часі. Реалізація даного методу дозволить підвищити оперативність виявлення програмно-технічного впливу та достовірність прийняття рішення про заходи щодо нейтралізації їх наслідків.

Напрямком подальших досліджень може бути повноцінна реалізація та налагодження даного методу мовою Go для ОС Astra Linux та проведення експериментів для вивчення та аналізу можливостей, характеристик та способів ефективного застосування різних типів нейромереж: LSTM, генеративно-змагальної нейромережі (GAN, generative adversarial network), керованого рекурентного блоку (GRU, gated recurrent unit) на вирішення завдання виявлення аномалій як реального часу.

Література:

1. Liu Hua Yeo, Xiangtong Che, Shalini Lakkaraju. Understanding Modern Intrusion Detection Systems: A Survey. URL: https://arxiv.org/ftp/arxiv/papers/1708/1708.07174.pdf (дата звернення: 22.12.2022).

2. Jain G., Sharma M., Agarwal B. Optimizing semantic LSTM for spam detection. *International Journal of Information Technology*. 2019. Vol. 11 (2). P. 239-250. DOI: 10.1007/s41870-018-0157-5.

3. Khoroshko V.A., Tkach Yu.N., Shelest M.E. Multialternative detection of cyberatacs in information networks. *Ukrainian Scientific Journal of Information Security*. 2021. Vol. 26, № 3, P. 136-141. DOI: 10.18372/2225-5036.27.16001.

4. Сучасні інформаційні технології в кібербезпеці: монографія / А.С. Довбиш, В.К. Ободяк, І.В. Шелехов та ін.; за ред. В.К. Ободяка, І.В. Шелехова. Суми: СумДУ, 2021. 348 с.

5. Рогоза П., Єсін В. Використання нейронної мережі замість бази знань у експертній системі детектору зловмисного трафіку до веб-ресурсів. *Комп'ютерні науки та кібербезпека.* 2022. № 1. С. 6-15. DOI: https://doi.org/10.26565/2519-2310-2022-1-01.

6. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник. Київ: ВІКНУ, 2016. 286 с.

7. Cyber digesto. Огляд подій в сфері кібербезпеки. URL: https://www.rnbo.gov.ua / files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber% 20digest_December_2022.pdf (дата звенення: 29.12.2022).

8. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/ (дата звенення: 25.12.2022).

9. Yin C., Zhu Y., Liu S., Fei J., Zhang H. An Enhancing Framework для Botnet Detection Using Generative Adversarial Networks. *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*. 2018. P. 228-234.

10. Yang Xin, Mingcheng Gao, Haixia Hou. Machine Learning and Deep Learning Methods for Cybersecurity. URL: https://www.researchgate.net/publication/325159145 (дата звернення: 29.12.2022).

11. Yin C., Zhu Y., Fei J., He X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*. 2017. Vol. 5. P. 21954-21961.

12. Jason Brownlee How to Develop LSTM Models for Time Series Forecasting. URL: https://machinelearningmastery.com/how-todevelop-lstm-models-for-time-series-forecasting/ (дата звернення: 10.01.2023).

13. Graves A. Generating Sequences with Recurrent Neural Networks. University of Toronto. URL: https://arxiv.org/pdf/1308.0850v5.pdf (дата звернення: 10.01.2023).

14. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/ (дата звернення: 28.12.2022).

References:

1. Liu Hua Yeo, Xiangtong Che, & Shalini Lakkaraju (2021). Understanding Modern Intrusion Detection Systems: A Survey. Retrieved from https://arxiv.org/ftp/arxiv/papers/1708/1708.07174.pdf [in English].

2. Jain, G., Sharma, M., & Agarwal, B. (2019). Optimizing semantic LSTM for spam detection. *International Journal of Information Technology, 11 (2),* 239-250. DOI: 10.1007/s41870-018-0157-5 [in English].

3. Khoroshko, V.A., Tkach, Yu.N., & Shelest, M.E. (2021). Multialternative detection of cyberatacs in information networks. *Ukrainian Scientific Journal of Information Security, 26 (3),* 136-141. DOI: 10.18372/2225-5036.27.16001 [in English].

4. Obodiaka, V.K., & Shelekhova, I.V. (Eds). (2021). *Suchasni informatsiini tekhnolohii v kiberbezpetsi: monohrafiia [Modern information technologies in cyber security: monograph]*. Sumy: SumDU [in Ukrainian].

5. Rohoza, P., & Yesin, V. (2022). Vykorystannia neironnoi merezhi zamist bazy znan u ekspertnii systemi detektoru zlovmysnoho trafiku do veb-resursiv [Using a neural network instead of a knowledge base in an expert system for detecting malicious traffic to web resources]. *Kompiuterni nauky ta kiberbezpeka – Computer science and cyber security, 1,* 6-15. DOI: https://doi.org/10.26565/2519-2310-2022-1-01 [in Ukrainian].

6. Kurban, O.V. (2016). *Suchasni informatsiini viiny v merezhevomu on-lain prostori: navchalnyi posibnyk [Modern information wars in the online network space: a tutorial]*. Kyiv: VIKNU [in Ukrainian].

7. Cyber digesto. Ohliad podii v sferi kiberbezpeky [Cyber digesto. Overview of events in the field of cyber security]. Retrieved from https://www.rnbo.gov.ua/ files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20digest_December_2022.pdf [in English].

8. European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/ [in English].

9. Yin, C., Zhu, Y., Liu, S., Fei, J., & Zhang, H. (2018). An Enhancing Framework для Botnet Detection Using Generative Adversarial Networks. *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 228-234 [in English].

10. Yang Xin, Mingcheng Gao, & Haixia Hou. Machine Learning and Deep Learning Methods for Cybersecurity. Retrieved from https://www.researchgate.net/publication/325159145 [in English].

11. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access, 5,* 21954-21961 [in English].

12. Brownlee, J. How to Develop LSTM Models for Time Series Forecasting. Retrieved from https://machinelearningmastery.com/how-todevelop-lstm-models-for-time-series-forecasting/ [in English].

13. Graves, A. Generating Sequences with Recurrent Neural Networks. University of Toronto. Retrieved from https://arxiv.org/pdf/1308.0850v5.pdf [in English].

14. Ministerstvo tsyfrovoi transformatsii Ukrainy [Ministry of Digital Transformation of Ukraine]. *thedigital.gov.ua*. Retrieved from https://thedigital.gov.ua/ [in Ukrainian].

Журнал

«Наука і техніка сьогодні»

(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)

Випуск № 1(15) 2023

Формат 60х90/8. Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 8,2. Наклад 100 прим.

Видавець:
Громадська наукова організація «Всеукраїнська асамблея докторів наук з державного управління»
Свідоцтво серія ДК №4957 від 18.08.2015 р., Андріївський узвіз, буд.11, оф 68, м. Київ, 04070.

Підготовлено рекламним агентством
«GoToPrint» Адреса, Україна, Київська обл.,
м. Київ, вул. Льва Толстого, 63
e-mail: gotoprint@gmail.com